

Forcepoint DSPM



Trasformazione dell'IA: il prossimo step della trasformazione digitale

In questa nuova era i tuoi dati sono al sicuro?

Le organizzazioni di tutti i settori si confrontano con la trasformazione dell'IA, spinta dalla promessa di un aumento drastico della produttività. Questa era potenziata dall'IA è caratterizzata da iniziative volte a introdurre servizi aziendali di IA, gestire l'uso non autorizzato dell'IA e mitigare i rischi associati all'attività di IA agentiva. In generale, una priorità fondamentale alla base di questi sforzi è la visibilità e il controllo sull'utilizzo dei dati sensibili. Tuttavia, praticamente ogni organizzazione fatica a ottenere una visibilità coerente, per non parlare del controllo, dei propri dati su larga scala. È come un iceberg, di cui vediamo solo una piccola parte in superficie, mentre la stragrande maggioranza rimane impercettibile sott'acqua. Questo fenomeno viene spesso definito "dark data" (dati oscuri): rimangono invisibili e sconosciuti, pur contenendo quantità significative di informazioni sensibili di cui l'organizzazione è direttamente responsabile. Ora, le organizzazioni stanno cercando di capire come consentire agli utenti di sfruttare l'IA in modo sicuro, garantendo al contempo la protezione dei propri dati sensibili; tuttavia, l'uso stesso dell'IA sta peggiorando il problema, poiché contribuisce a creare una quantità di dati sempre maggiore a una velocità senza precedenti.



Data Security Posture Management (DSPM) offre un approccio completo per proteggere le Sue informazioni da accessi non autorizzati, divulgazione, alterazione o distruzione dei dati. A differenza di altri metodi di sicurezza dei dati incentrati su applicazioni e dispositivi specifici, DSPM è in grado di visualizzare e controllare l'intero patrimonio di dati di un'organizzazione, sia nel cloud che su reti private, garantendo la conformità e mitigando il rischio di violazioni dei dati.



Percentuale di organizzazioni che ha segnalato una violazione legata all'IA e non disponeva di controlli di accesso all'IA adeguati.¹



Risparmi sui costi grazie all'uso estensivo dell'IA nelle operazioni di sicurezza. I team di sicurezza che utilizzano ampiamente l'IA e l'automazione hanno ridotto i tempi di contenimento delle violazioni di 65 giorni e abbassato i costi medi di 1,93 milioni di dollari USA rispetto a chi non ha utilizzato queste soluzioni¹.



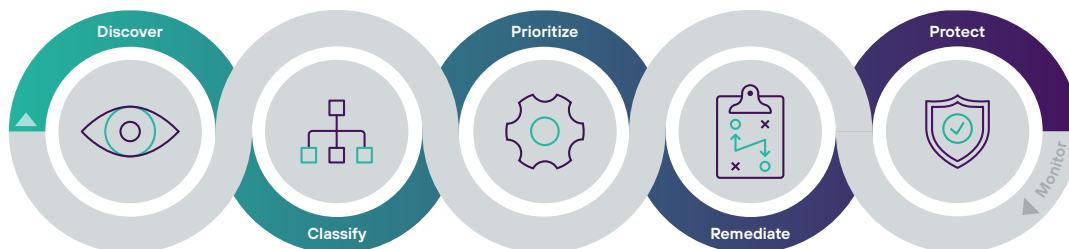
AT&T ha accettato di pagare 177 milioni di dollari per chiudere un'azione collettiva legata a due violazioni avvenute nel 2024. La prima violazione ha esposto dati, inclusi i numeri di previdenza sociale, di 73 milioni di clienti attuali ed ex clienti, mentre la seconda ha riguardato l'accesso non autorizzato a un'area di lavoro contenente informazioni sensibili dei clienti, ospitata in un ambiente cloud privo di un monitoraggio adeguato².

¹ IBM's Cost of a Data Breach Report 2026
² Top Class Actions accordo transattivo dell'azione collettiva relativa alla violazione dei dati di AT&T

Cosa fa DSPM?

- **Percorso di trasformazione dell'IA:** libera il potenziale dell'IA con Forcepoint DSPM, salvaguardando i dati ovunque grazie alla nostra avanzata tecnologia AI Mesh. Con la visibilità e la risoluzione centralizzata da Forcepoint DSPM e i controlli di blocco in tempo reale da Forcepoint DLP, proteggiamo le tue informazioni sensibili attraverso i canali chiave, tra cui le applicazioni dell'IA generativa come ChatGPT, Copilot, Gemini e molti altri, potenziando l'innovazione audace e aumentando la produttività e riducendo il rischio.
- **Identificazione dei dati sensibili:** DSPM aiuta le organizzazioni a identificare i dati sensibili attraverso più ambienti e servizi cloud e le sedi on-prem, inclusi i dati strutturati e non strutturati. Ciò include la comprensione di dove risiedono i dati sensibili, come si accede e chi ha le autorizzazioni per interagire con essi.
- **Valuta la vulnerabilità e il rischio:** DSPM valuta la vulnerabilità dei dati sensibili alle minacce alla sicurezza e il rischio di mancata conformità alla normativa. Analizzando la posizione di sicurezza dei dati, le organizzazioni possono affrontare proattivamente i potenziali rischi.
- **Si concentra sui dati alla fonte:** a differenza di altri strumenti di sicurezza dei dati che proteggono principalmente dispositivi, sistemi e applicazioni, DSPM si concentra direttamente sulla protezione della totalità dei dati di un'organizzazione. Mira a prevenire le violazioni dei dati e a garantire la conformità proteggendo i dati al centro.
- **Gestisce i dati oscuri e i dati ROT:** DSPM interviene direttamente sui dati oscuri (dati attualmente non visualizzati o non utilizzati nei normali processi aziendali). Analogamente, DSPM è in grado di rimediare i dati ROT (dati ridondanti, obsoleti e banali), i quali solitamente proliferano nelle organizzazioni man mano che si accumulano i dati conservati per varie ragioni, nella convinzione che ciò contribuisca alla conformità. In realtà, crea un rischio ancora maggiore per i dati e DSPM aiuta a gestire tale rischio.
- **Identifica e corregge i dati con autorizzazioni/esposizione eccessive:** a causa del modo in cui i dati proliferano mediante la copia e la modifica di nuove versioni dei dati, spesso i dati possono estendersi a utenti, gruppi e persino all'intera organizzazione. DSPM aiuta a far rispettare il concetto di Zero Trust del "principio del privilegio minimo", che riduce drasticamente i dati con autorizzazioni eccessive al fine di prevenire le violazioni dei dati.
- **Ambienti multi-cloud e cloud ibridi:** con la crescente adozione di ambienti multi-cloud e cloud ibridi, il rischio di violazioni dei dati aumenta drasticamente. DSPM offre visibilità e controllo sui dati sensibili nei diversi ambienti di elaborazione oltre alle sedi locali.
- **Monitoraggio continuo del rischio:** il componente aggiuntivo di Forcepoint Data Detection and Response (DDR) consente a Forcepoint DSPM di rilevare e porre rimedio ai nuovi rischi per i dati nel momento in cui si verificano. Non è necessario attendere la prossima scansione DSPM completa: identifica dinamicamente i rischi per la posizione di sicurezza dei dati per porvi rimedio.

Forcepoint DSPM è progettato per le organizzazioni moderne che hanno bisogno di visibilità e controllo sui dati sensibili. Fornisce visibilità in vari ambienti cloud e server per prevenire le violazioni di dati e ridurre il rischio di mancata conformità rispetto alle normative sulla privacy. Forcepoint offre visibilità e controllo lungo l'intero ciclo di vita dei dati, proteggendo i dati ovunque, combinando il **rilevamento proattivo del rischio dei dati** (DSPM) con **controlli attivi sul modo in cui questi vengono utilizzati** (DLP) e **adattandosi continuamente alle azioni di ciascun utente** (Risk-Adaptive Protection). Ottieni la scoperta dinamica del rischio dei dati con il monitoraggio continuo (Forcepoint DDR) per prevenire le violazioni dei dati e proteggere la tua sicurezza dei dati.



Discovery, classificazione e orchestrazione basati sull'IA

Unisci visibilità e controllo sul panorama dei tuoi dati con Forcepoint DSPM

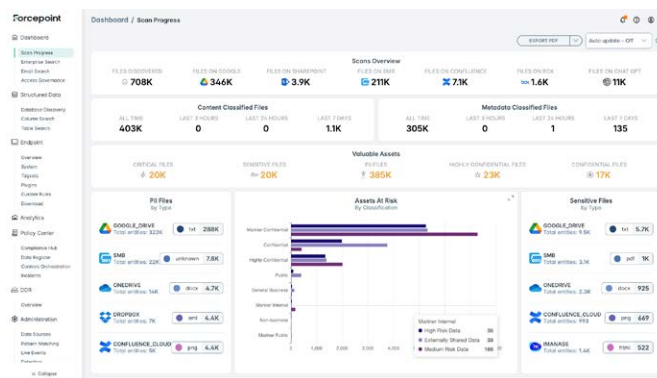
Gestire e proteggere i dati della Sua organizzazione non è mai stato così complesso. Forcepoint DSPM offre una soluzione potente per ottenere una visibilità e un controllo completi sui Suoi dati, indipendentemente dalla loro posizione. Grazie a una classificazione dei dati all'avanguardia basata sull'ispezione completa dei contenuti, resa possibile dall'AI Mesh di Forcepoint e da classificatori DLP avanzati, Forcepoint DSPM Le consente di prendere decisioni informate sulla Sua postura di sicurezza dei dati e di affrontare in modo proattivo i potenziali rischi.

I principali vantaggi di Forcepoint DSPM includono:

Scoperta rapida e completa: Forcepoint DSPM esegue una scansione rapida e ad alte prestazioni di file e database in ambienti multicloud e on-premise, effettuando un'ispezione completa dei contenuti anziché affidarsi al semplice tagging dei metadati o ad approcci basati sul campionamento. Questo livello di analisi garantisce che i dati sensibili vengano identificati con precisione, non semplicemente stimati. L'individuazione e la classificazione ad alte prestazioni di Forcepoint consentono alle organizzazioni di ottenere una visibilità rapida e completa sul proprio panorama di dati su larga scala, comprendendo sia i repository strutturati che non strutturati, inclusi i dati residenti su piattaforme di IA generativa come ChatGPT Enterprise, Anthropic Claude e Microsoft Copilot, aiutando i team di sicurezza ad anticipare i rischi emergenti di esposizione dei dati legati all'IA.

Precisione basata su AI Mesh: Forcepoint DSPM individua i dati tra le fonti cloud e di rete e li classifica automaticamente utilizzando un motore avanzato di classificazione basato sull'IA. L'AI Mesh di Forcepoint DSPM offre alle organizzazioni una precisione di classificazione dei dati superiore. La sua architettura

di IA in rete, che sfrutta un Small Language Model (SLM) GenAI e i classificatori DLP di Forcepoint, affidabili da tempo e accuratamente selezionati, cattura in modo efficiente il contesto da testo non strutturato. Personalizzabile ed efficiente, garantisce una classificazione rapida e precisa senza richiedere un addestramento estensivo, migliorando fiducia e conformità. In definitiva, questa elevata precisione ha permesso alle organizzazioni che avevano riscontrato difficoltà con altri metodi di classificazione diffusi di ridurre drasticamente i falsi positivi/negativi, proteggendo con successo la propria proprietà intellettuale e risparmiando ingenti quantità di tempo e risorse.



Visibilità su tutto il panorama dei dati: Forcepoint DSPM consente di ispezionare le autorizzazioni per tutti i file e gli utenti. Gli amministratori dei dati possono vedere quali individui hanno accesso a file e database in tutta l'organizzazione. Con un solo clic è possibile visualizzare immediatamente le autorizzazioni per tutti i file scansionati. Forcepoint DSPM fornisce una dashboard con dettagli approfonditi che offrono una visione a volo d'uccello sui dati oscuri e forniscono una valutazione panoramica del rischio dei dati per aiutarti a comprendere le aree a più alto rischio per i dati.

Orchestrazione del flusso di lavoro: definisci facilmente la proprietà e la responsabilità per diversi set di dati per facilitare l'allineamento tra i vari stakeholder. Ciò consente flussi di lavoro più efficienti sulle azioni eseguite su ciascuna fonte di dati e risorsa. Una riparazione effettiva richiede un ampio coinvolgimento e una collaborazione oltre all'organizzazione della sicurezza per il gruppo CDO/Governance o Risk & Compliance (GRC)

nonché funzioni come marketing, finanza, DevOps e molto altro. Forcepoint DSPM considera la protezione dei dati non solo come un problema di sicurezza, ma come una priorità del business.

Forcepoint DDR: una potente aggiunta a Forcepoint DSPM, rappresenta una soluzione chiave per affrontare le violazioni dei dati. Fornisce il rilevamento continuo della minaccia e una visibilità avanzata del rischio dei dati, garantendo che le organizzazioni possano vedere efficacemente le modifiche ai dati che probabilmente portano a violazioni dei dati man mano che si verificano. Sfruttando risposte basate sull'IA, Forcepoint DDR offre una precisa neutralizzazione delle minacce, aiutando le organizzazioni a mantenere solide misure di sicurezza. La sua ampia visibilità su cloud ed endpoint, combinata con il tracciamento della provenienza dei dati, lo rende uno strumento essenziale per proteggere le informazioni sensibili, ridurre le perdite finanziarie e mantenere la fiducia dei clienti.



Non lasciare che i dati a rischio paralizzino la tua azienda. Forcepoint può aiutarti

Nell'era digitale di oggi, i dati sono un patrimonio prezioso per le organizzazioni, ma possono anche diventare un onere, se non vengono gestiti correttamente. Forcepoint DSPM offre un approccio proattivo per proteggere i dati sensibili, mitigare i rischi di violazioni e garantire la conformità alle normative. Implementando Forcepoint DSPM, puoi ottenere una visibilità completa sul tuo panorama dei dati, individuare e risolvere le vulnerabilità e proteggere in modo proattivo la tua organizzazione dagli eventuali danni finanziari e reputazionali causati da violazioni dei dati e dalla mancata conformità alle normative, proteggendo al contempo i tuoi dati nelle applicazioni GenAI. Prendi il controllo della tua posizione di sicurezza dei dati oggi stesso. Scopri come la soluzione DSPM può proteggere le tue preziose informazioni. Vai su www.forcepoint.com/it/dspm per richiedere una demo.



[forcepoint.com/contact](https://www.forcepoint.com/contact)

About Forcepoint

Forcepoint offre Self-Aware Data Security, un approccio nativo dell'IA che aiuta aziende e governi a conoscere i propri dati ovunque si trovino, ad adattarsi in tempo reale all'evoluzione dei rischi e delle normative e a garantire una protezione su larga scala grazie a un framework unificato basato su un'unica policy. Con sede ad Austin, in Texas, Forcepoint crea ambienti sicuri e affidabili per i clienti e i loro dipendenti in oltre 150 Paesi. Segui Forcepoint su www.forcepoint.com, [LinkedIn](#), [Instagram](#) e [YouTube](#).